Keynote talk for S4x16 by Mikko Hypponen.

Hello. I am Mikko Hypponen. I'd like to talk to you about the world where we live in.

Here we are facing another year. Behind us lies 2015, one of the most confusing, disturbing and politically complicated years we have seen in decades. Technologies have always played an important role in such complications. And technology has always played an important part in conflict.

But no technology has been more relevant to conflict than the internet. And today I'd like to show you why.

Chapter 1 - a world becoming

In the beginning was the world. A virgin world: a world without us and without technology. Nature came along: made plants and trees and insects and animals. After series of experiments, it eventually got around to making us. Humans.

Humans, it would appear, were deeply dissatisfied with what this world had given them and set about trying to rectify the shortcomings of Mother Nature. We sharpened stones, cut down trees, made weapons and made homes. We hunted.

Humans even developed the skill of speech so that they could tell each other how unhappy they were with the general state of things. If someone else disagreed with them, then they cut down more trees and sharpened more stones so they could convince others of their argument.

Humans discovered fire, burned meat, and made things out of metal. They had Gods: lots of Gods. Gods that mastered elements, fears, politics and wars. These Gods had churches, temples, high priests and inquisitions: and they would go on to battle another new church - the church of science.

Humans wandered the planet, spreading language, technologies and belief systems: cities grew out of dust and the cities had walls with big doors to keep people out and people in. The walls were there to protect and suppress. The walls were a level of security for the people and for the state. There was incredible wealth and unimaginable poverty and through all of this is the undeniable connection between control and power, between fear and technology.

Chapter 2 - infrastructures at war

The walls around cities become higher, longer and wider. The longer and wider these walls, the more invisible they became, marking areas of wealth, prosperity and power and, in some cases, fear.

Eventually these walls became borders. They became invisible fences of ownership, enabled by the craft of map-making. Many of these borders remain today. Many have disappeared by the hand of nature and others still lost and won through wars.

The staggering possibilities of technology always seem to shine at their strongest during periods of war. And most early wars were over the ownership of land and the shifting of borders.

Traditionally, conflicts arose around one group of people wanting something that another group of people had. Or one group of people was odds with the belief systems of another group. War is what happens when words and diplomacy fail. Thousands of years of conflict have made humans very good at making things for war.

War has been a real driver of technology. And technology has driven war. Gunpowder, tempered steel blades, muskets and cannons are technologies of war. The British won the battle of Agincourt in 1415 even though they were woefully outnumbered. They did not win because they were stronger. They did not win because Henry V was a smarter military tactician. They won because they had better technology. They won because they had the long bow and arrows.

WW1 & WWII.

World War I and World War II were technology accelerator labs. We found new and improved ways of attacking enemy infrastructures. We found new ways of causing havoc. The brightest minds were taken from their universities to develop weapons of mass destruction.

The Second World War was also the first time a computer was used to attack a foreign military objective. Granted, we aren't speaking about cyberwarfare, but about breaking the encryption that was used to protect military communications. Nevertheless, computer age started with a world war. Jet engines, chemical weapons, plastic explosives, radar, rocketry and a host of other technologies were developed and had a lasting effect upon the lives we live today.

But one development changed and determined the course of geopolitics for the over sixty years. And that was the development of the atom bomb.

Cold War and the Internet.

The atom bomb split the world in two. The Iron Curtain was a new kind of border. It was a border of things. Things like the arms race, the cold war, espionage, counter intelligence, information warfare and the Berlin wall. Those of us who remember a life during the cold war will recall the constant fear of imminent disaster. Our world could end any minute.

For soldiers, invention of the nuclear weapon was like a gift from heavens. What could be more excellent than nuking your enemy, a thousand miles away and from the comfort of your own bunker? Too bad that the enemy has the same bombs too! The Cold War was a glorious time for war because, never in the history it was so obvious who was the enemy. The enemy was clear. The borders that were must not cross were clear. And the means of war were clear too. If there was going to be a war, it would be fought with nuclear weapons.

We were living in a constant state of fear: we even had a fear meter. It was called a DEFCON meter – a Defense Readiness Condition meter, not the party in Las Vegas. DEFCON would tell us how close we were to Armageddon.

One of the side effects of the cold war was that the internet was created. US military created is at a way to uphold a chain of command during nuclear war. The Internet was created as a military infrastructure. By developing the Internet, mankind opened up a whole new way of waging war on one another. And the internet has no geography. It was no borders. By creating the internet, the mankind opened up a Pandora's Box where tangible borders and recognizable enemies ceased to exist.

We should also note that the power of nuclear weapons was mostly in deterrence. The human kind has only used a nuclear weapon in war twice in history. The rest of the power of nuclear weapons has been in deterrence. The power has been in knowing who has the weapons. And we know who has the weapons because they were openly testing them. Even today, it's trivial to list who has nuclear weapons. USA, Russia, UK, France, China, India, Pakistan, North Korea and Israel. That's it. And we know they have nuclear weapons because they test them.

The difference between nuclear arms race and cyber arms race is that in cyber arms race we have no idea who has what. For example, what's the offensive online capability of Vietnam? Or South Africa? Or Brazil? Do you know? Because I sure don't. So the power of future cyber arms is definitely not in deterrence. And this new arms race is just starting. I believe that we've only seen the very beginning of the cyber arms race. The race is on because these new kinds of weapons make sense. They are cheap, accessible and deniable. That's a great combo.

Technology of war has moved on. We no longer know, or can clearly describe who the enemy is, what they want to achieve, or what their motives are. We go into battle using technologies we don't fully understand, against enemies that remain in the shadows and on into wars that we will never know if they are over or not. Who is the enemy? Hackers? Anonymous? The Russian Mafia? North Korea? ISIS?

Chapter 3 - world war i

So, what could happen today? What could be possible? What could be doable?

Let's take an example. How about an attack against, say, a Coca Cola bottling plant in the United Kingdom?

Over 97% of all Coca Cola products produced for the British Market are bottled in Wakefield, Yorkshire, pretty much dead center in the United Kingdom. They bottle a 40.000 bottles an hour. They have invested £52 million in plants across Great Britain. 52 million pounds. That's a lot of money. With today's exchange rate that…I don't know. About 500 dollars? Anyway, they've invested a lot in their technology. And details of their machinery and their plant locations are available to anyone with a simple google search. Linkedin lists dozens of their key employees.

With that kind of information, their operations could be targeted in various ways. But why? Why would anyone want to disrupt a company like Coca Cola?

A company like this could become a target just because it's so big. Because it's so visible. And because it stands for something. What's more American than Coca Cola? What's a better

symbol for capitalism? What's a better symbol for wealth? If you attack Coca Cola, you attack everything that the brand stands for. You attack everything that America stands for.

A company like this could also be attacked for financial benefit. For stealing corporate data. Or to be held for ransom. The visibility of a disruption for a company like this would be significant. Imagine coke not being able to deliver drinks over the Christmas holidays, for example.

The most important underlying technology for everything around us is, quite simply, electricity. That's why it really should be the most important resource we need to be protecting. Without electricity, they wouldn't be able to bottle coca cola. In fact, without electricity, we wouldn't be able to feed our people.

Our next conflict will be one without borders. Our next conflict will be fought against people that have motivations that are hard for us to understand.

In the past there were enemies and allies. In the past people were with us or against us. In the past fighters wore uniforms and had flags to show off their allegiance.

In future conflicts, groups came and go and joint attacks are made. Extremists can team up with hackers. Hackers team up with fanatics. And fanatics team up with criminals.

We already know from bitcoin blockchain traffic that some of the Russian ransomware gangs have made several hundreds of millions of dollars. Hundreds of millions of dollars. So the question is: do we already have cybercrime unicorns? Cybercrime unicorns. Sure is strange.

ICS

Everything in the world of industrial control systems is global. So, how does a plant in Japan trust the PLCs they bought from a Germany? Or the routers they bought from China? Or the workstations they bought from USA? Or the security system they bought from Russia? That's a great question, isn't it? After all, you must choose a vendor. Either you choose a vendor or you don't operate at all.

One of the reasons we are asking these questions today is Mr. Snowden. His exposes on the overreach of the US intelligence agencies were staggering. Learning that the NSA actually does intercept Cisco routers while they are being shipped to international customers so they can insert backdoors is a pretty big deal.

And there's plenty of bad news that did not come from Mr. Snowden. For example, the Flame malware was most likely created by a US intelligence agency, and to spread it to their targets, the attackers used Windows Update. Which means that the most critical network of the largest software vendor in the United States was attacked by their own government. It sure is strange.

Siemens controls a very large part of the PLC market, and we know it was their systems that were circumvented by Stuxnet. We keep finding vulnerabilities from critical routers created by Huawei. Although, as a friend of mine said after reverse engineering a large part of one of their routers: there's no way to say if this box is vulnerable on purpose or if it's just shitty code.

Reboot

As ICS customers, we need to know the policies our vendors have related to their relationships with their own governments and their intelligence agencies. Clever vendors actually make their policies on this public to the world. Knowledge like this is needed if we want there to be trust.

And it all boils down to trust.

Trust. That's a complicated word in the internet age.

Let me tell you about trust.

I'm from Finland. Finland is a country the size of California, but it only has 5 million people. We share a thousand mile border with Russia. Russia is the largest country on the planet and has 150 million people.

In 1939, when Russia started invading Finland, it was quite obvious to everyone we couldn't possible win the fight. The only sensible thing Finland could do was to surrender without a fight. But we didn't. It might have made no sense, but we fought them anyway. Both of my late grandfathers were there, over 70 years ago, fighting the Russians. And, as the result, unlike the rest of the Eastern Europe, Finland kept her independence.

After the war, both my grandfathers hated the Russians. They absolutely hated them. They would have never trusted a Russian. And who could blame them. My father? He doesn't hate the Russians. But he doesn't like them either. Me? I don't hate the Russians at all. It's a country full of great people and great talent. I've hired a lot of Russians programmers and researchers over the years. And I trust many Russians personally, after getting to know them. I might not trust the government of Russia, but I do trust many Russians.

However, I definitely do not trust the Russian intelligence agencies, and I definitely do not trust President Putin. Why would I? Trust has to be earned, and they definitely haven't earned mine.

End

As I said in the beginning, behind us lies one of the most confusing, disturbing and politically complicated years we have seen in decades. But I have hope for the future. I believe in reboots. I believe in redemption. I believe in recovery.

German philosopher Herbert Marcuse has said that the needs and greed, the hopes and fears of the inventor of a piece of technology become part or the aura of that technology. We're in the middle of a borderless war being played out on technical infrastructure whose aura is that of fear and a deep mistrust of the enemy.

We should be replacing systems, technologies and thinking steeped in fear, suspicion and mistrust with - infrastructures based on trust.

Without safety we won't have security.

Without security we won't have trust.

And without trust, we won't have anything at all.

We all here work with security. It is our job to do the best we can to prevent our own governments and our own politicians from eroding the trust in the technology our country builds and exports.

It is our job to explore, define, understand and help oversee this new borderless landscape and to protect it.

This is our job. It's our job to understand the cyber geopolitics.

We're needed now. We're needed to be building trust.

And we need to be building it together.

Thank You for being here.

Thank You for your work.

Thank You.